Secure Access with 802.1X

Configuration, deployment and troubleshooting

Session 619

These are confidential sessions—please refrain from streaming, blogging, or taking pictures.

At the convention center, a movie will be placed here

Secure Access with 802.1X

Configuration, deployment and troubleshooting

Tommy Hann
Consulting Engineer

Introduction

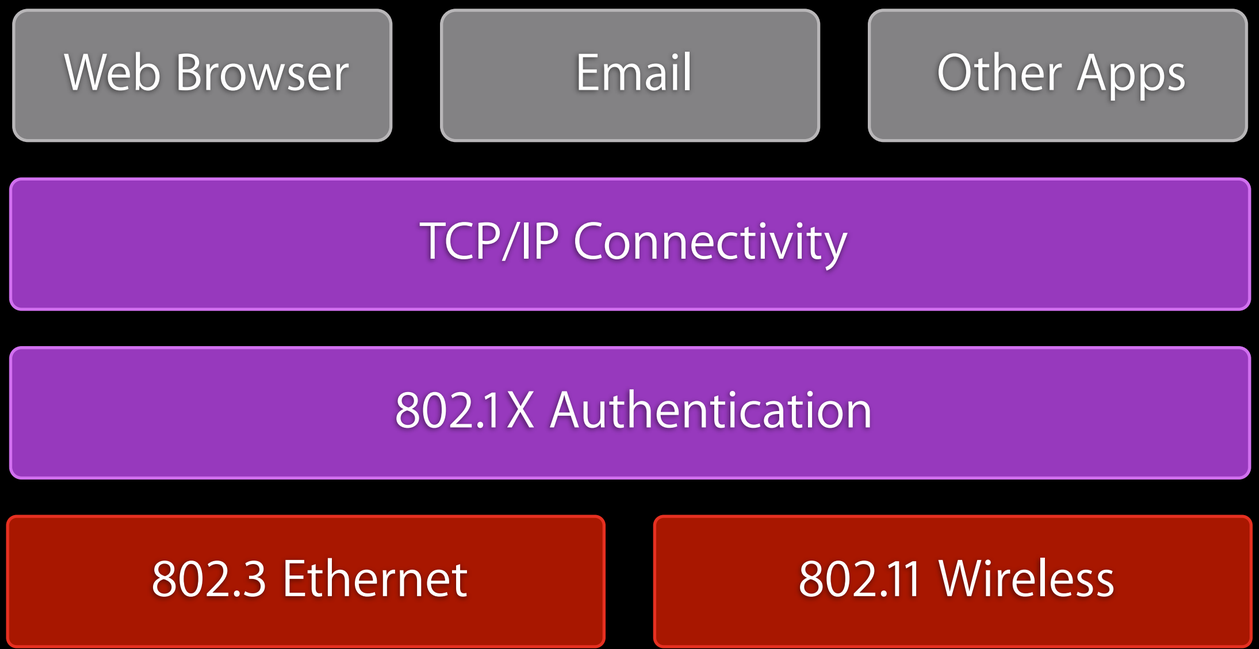
- IEEE 802.1X: Port-based network access control (authentication)
- Wi-Fi Alliance requires 802.1X for enterprise wireless security
- 802.1X is becoming commonplace for wireless security
- Isn't WPA/WPA2 PSK good enough?
- 802.1X may be used for wired security as well
- Built-in Mac OS X Supplicant
- Built-in iPhone OS Supplicant
- RADIUS service in Mac OS X Server (802.1X Authentication Server)

Agenda

- IEEE 802.1X overview
- Mac OS X Server RADIUS
- Configuration of Mac OS X and iPhone OS
- Deployment strategies
- Troubleshooting
- 802.1X demo
- Q&A

802.1X Authentication Layer

Conceptual layers



IEEE 802.1X Overview

IEEE 802.1X for Network Authentication

- Port-based network access control (authentication)
- At the point of network attachment
- Authentication via EAP (Extensible Authentication Protocol)
- Commonly utilizes PKI (Public Key Infrastructure)

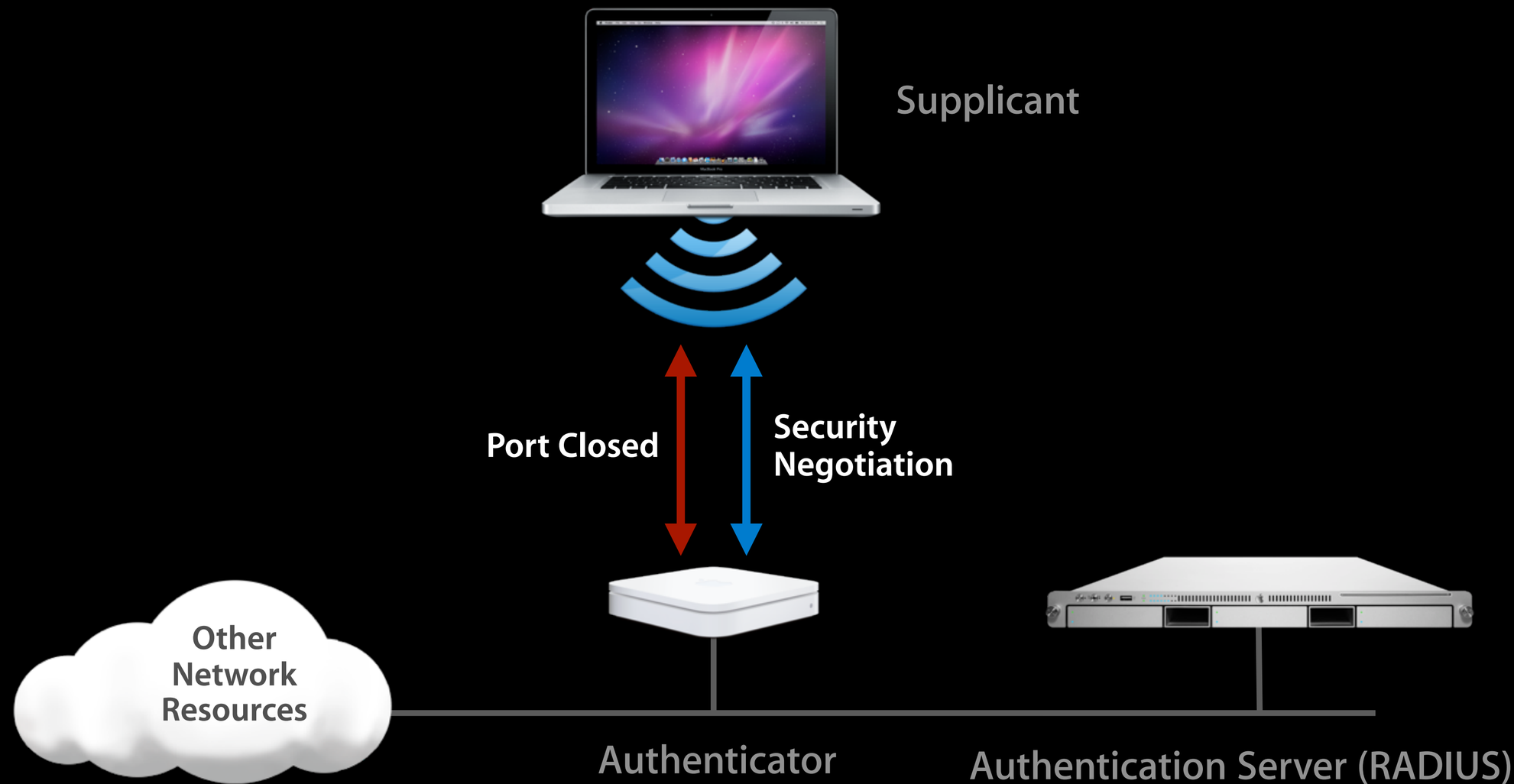
- Mutual authentication between client and server

Supplicant

Authenticator

Authentication Server (RADIUS)

Port-based Network Authentication

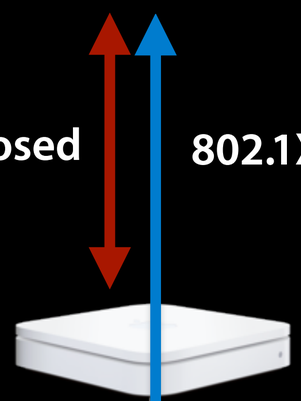


Port-based Network Authentication

Supplicant

Port Closed

802.1X Authentication

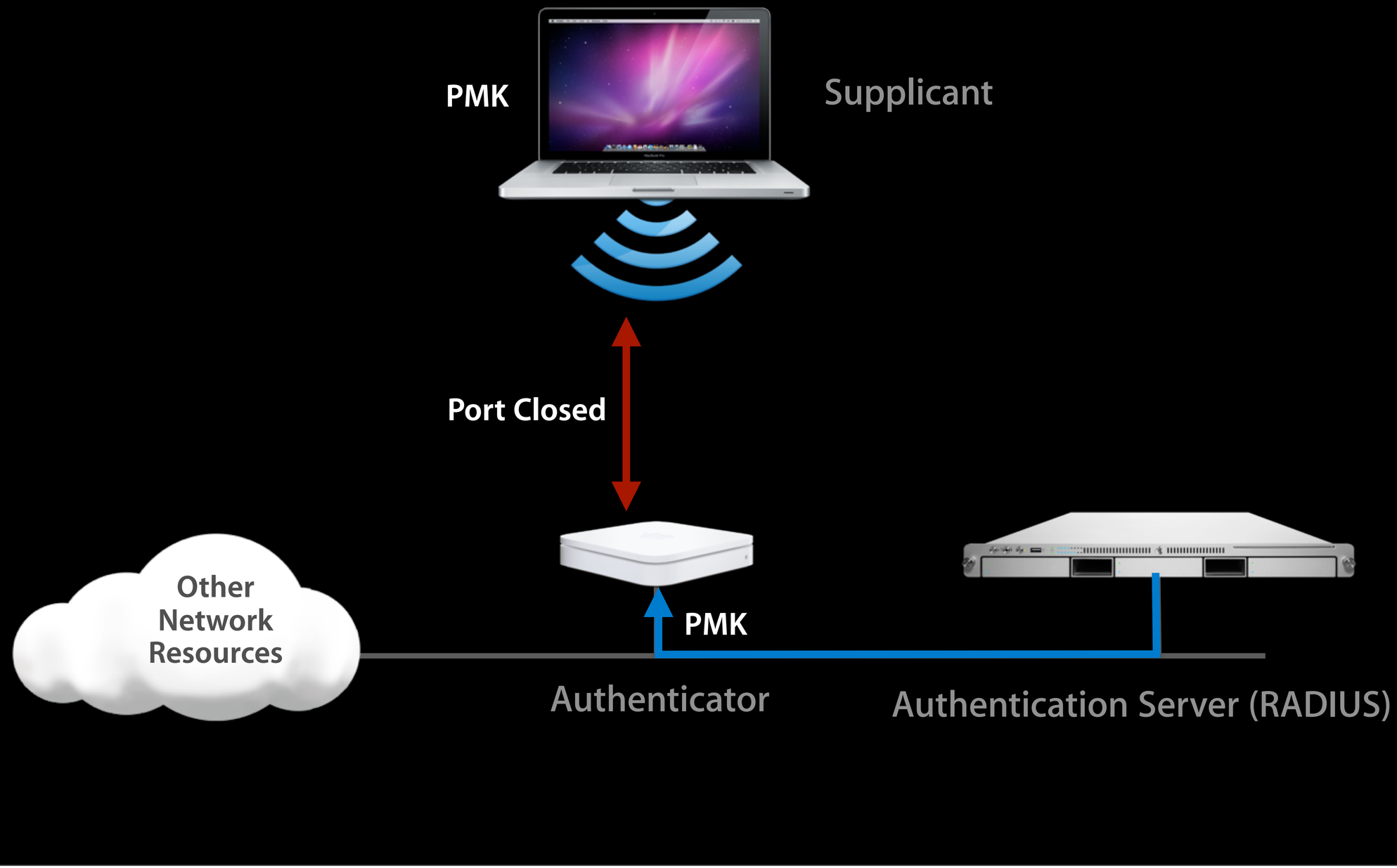


Other Network Resources

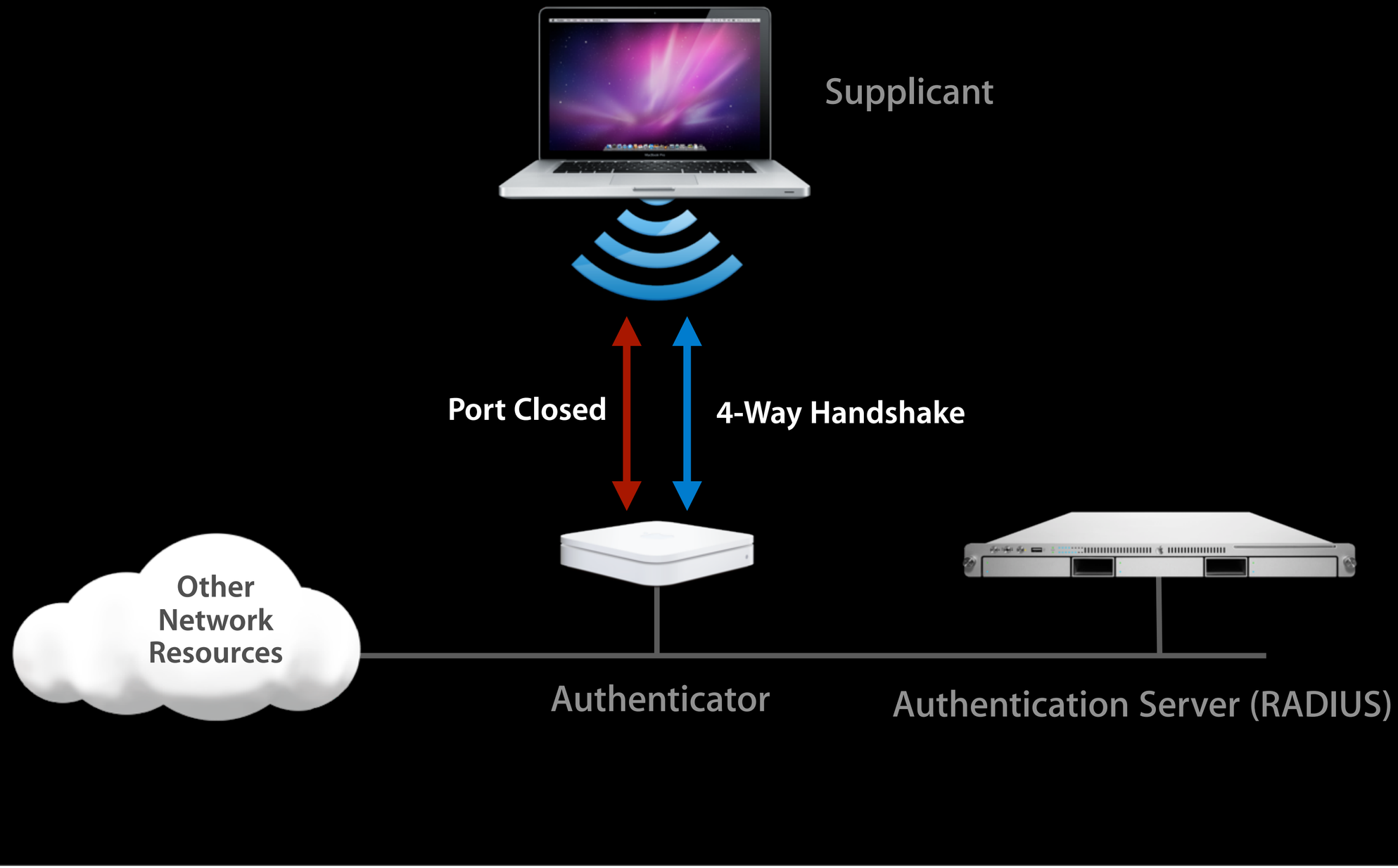
Authenticator

Authentication Server (RADIUS)

Port-based Network Authentication



Port-based Network Authentication



Port-based Network Authentication

Supplicant

Port Open
Data Encrypted

Other Network Resources

Authenticator

Authentication Server (RADIUS)

802.1X EAP Types

EAP—Extensible Authentication Protocol

- EAP-TLS: Transport Layer Security
- EAP-TTLS: Tunneled Transport Layer Security
- PEAP: Protected Extensible Authentication Protocol
- EAP-MD5: Message Digest Algorithm
- LEAP: Lightweight Extensible Authentication Protocol
- EAP-FAST: Flexible Authentication via Secure Tunnel
- EAP-SIM: Subscriber Identity Module

802.1X and PKI

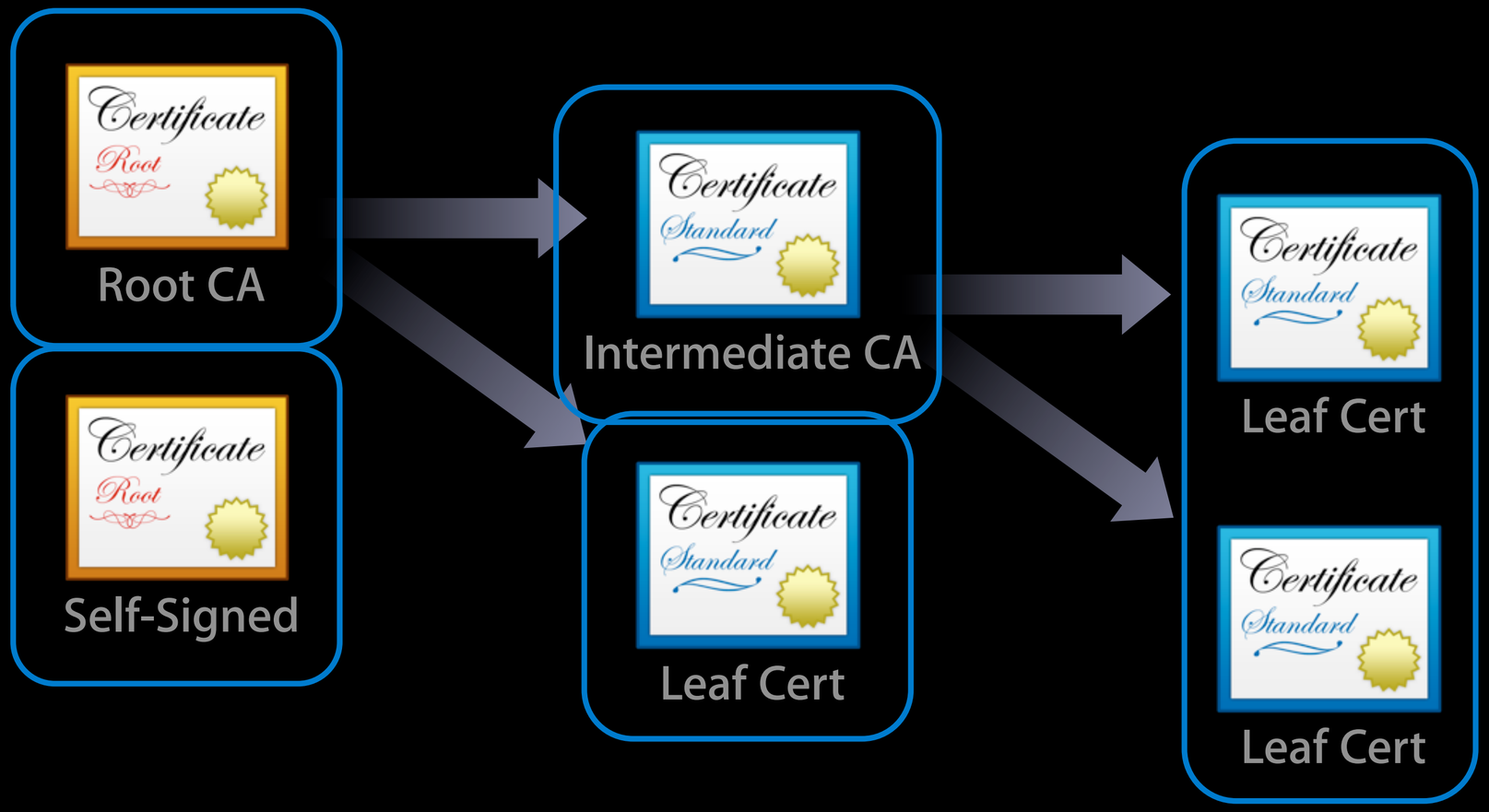
PKI—Public Key Infrastructure

- Optional client-side certificate for user or computer authentication
- Server-side certificate for server authentication
- No correlation between SSID and domain name
- Must explicitly trust server certificate chain

802.1X and PKI

PKI—Public Key Infrastructure

- Explicit trust at any level



Wired 802.1X

802.1X is not just for wireless

- Used to protect ethernet jacks in public locations
- Challenge compared to wireless
  - Doesn’t know network is protected
  - Similar to 802.1X WEP—Is it WEP or 802.1X WEP?
- Dynamic VLAN switching

Mac OS X Server

Snow Leopard Server-RADIUS

RADIUS used for 802.1X authentication server

- FreeRADIUS version 2.1.3
- GUI for configuration
- Five minutes and RADIUS is up and running
- Integrated with Directory Services
  - Open Directory authentication
  - Active Directory authentication
- Command line configuration via ‘radiusconfig’

Mac OS X Supplicant

802.1X Modes

Mac OS X implementation

- User mode
- System mode
- Login window mode
- Mixed mode (new in Snow Leopard)

802.1X Modes

Mac OS X implementation

- User mode
  - Authentication sessions started as the logged-in user
  - Information from user's preferences and keychain
- System mode
  - Authentication session started by the system, regardless of user
  - Information from system preferences and keychain

802.1X and an External Directory

Login window mode: The chicken and the egg

A network user must authenticate against the directory server to log in

To reach the directory server, the computer must have network access via 802.1X

To authenticate via 802.1X, the user must already be logged into the computer

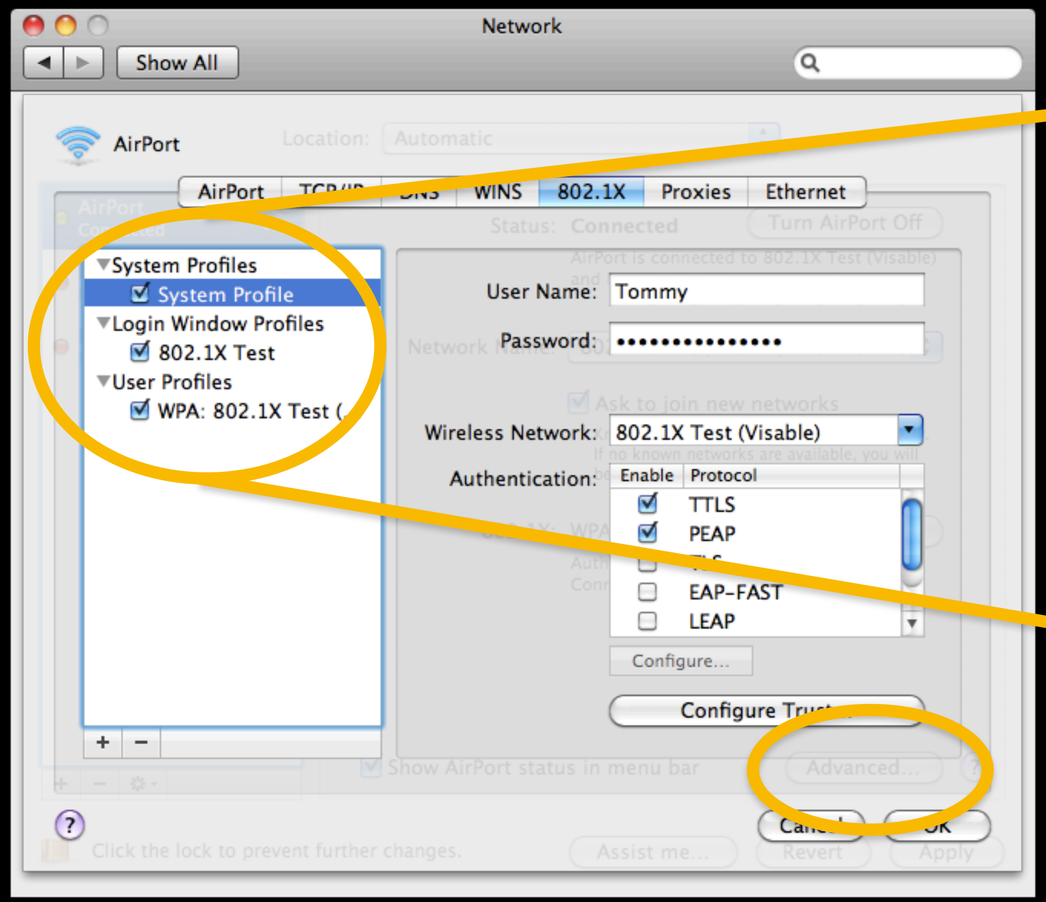
802.1X Modes

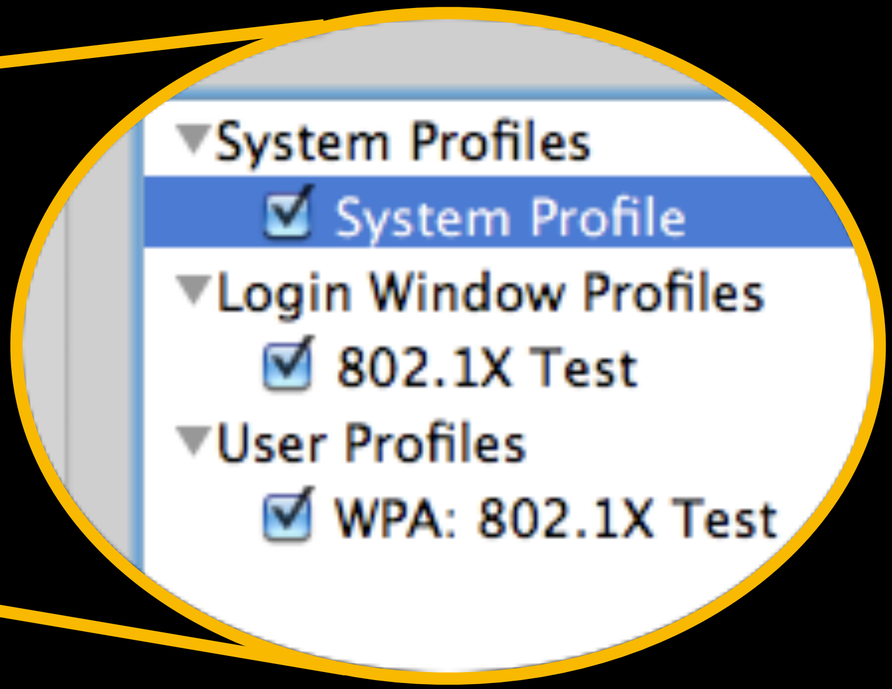
Mac OS X implementation

- Login window mode
  - Used in conjunction with an external directory
  - Authentication session started by login window
  - Credentials from login window system preferences and keychain
- Mixed mode
  - New in Snow Leopard
  - Common example:
    - System mode for machine authentication
    - Login Window mode for user authentication

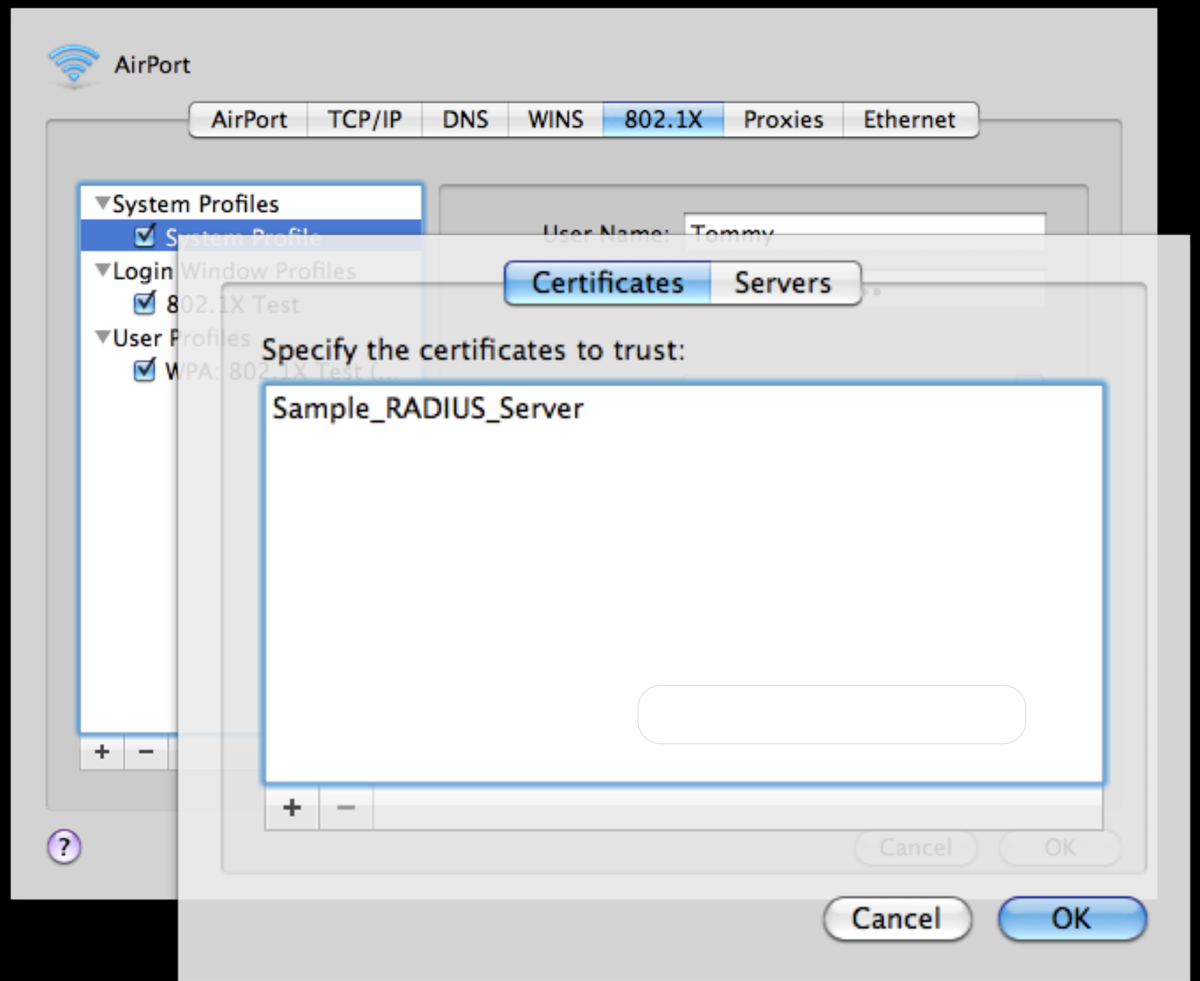
802.1X Profile Types

Mac OS X implementation





Certificate Trust



- Certificates stored in keychains
- Explicit trust at any level
- New Snow Leopard trust GUI
  - Certificate trust
  - Server trust
- Command line: /usr/bin/security

```
security dump-trust-settings -d
```

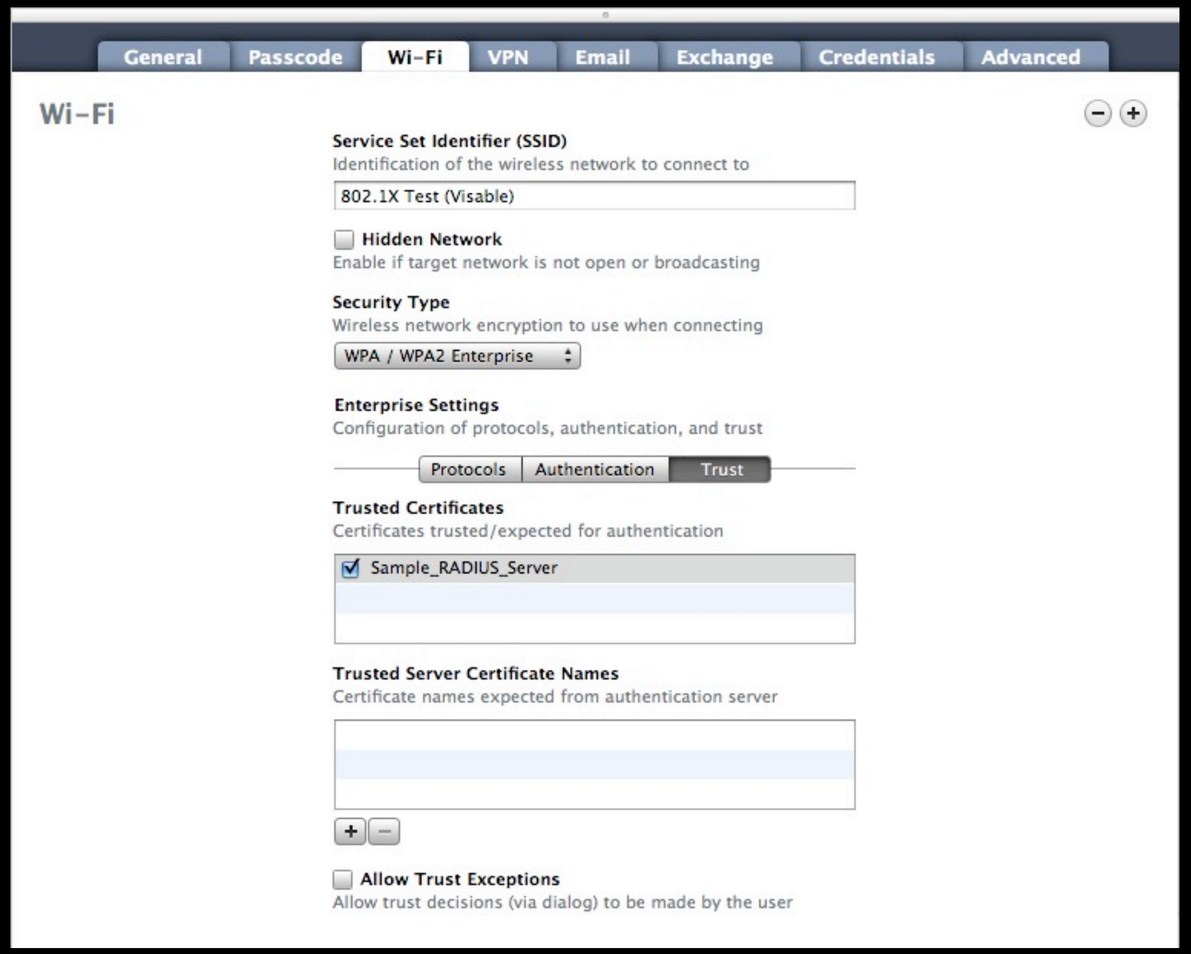
Demo

iPhone OS Supplicant

Single 802.1X Mode

iPhone OS

- Only one profile type-user profile
- Connection similar to OS X
- “Automatic” profile template
- Certificate trust similar to OS X
- Certificate trust
  - Dynamic
  - Tied to SSID
- Autojoin similar to OS X
- Forget network to stop autojoin and remove certificate trust



Custom Profiles

iPhone OS

- iPhone Configuration Utility
- Profile creation
- Explicit certificate trust
- User/machine identity (PKCS12)
- Trusted (signed) profiles
- Autojoin on/off switch

Demo

Deployment Strategies

Importing/Exporting Profiles

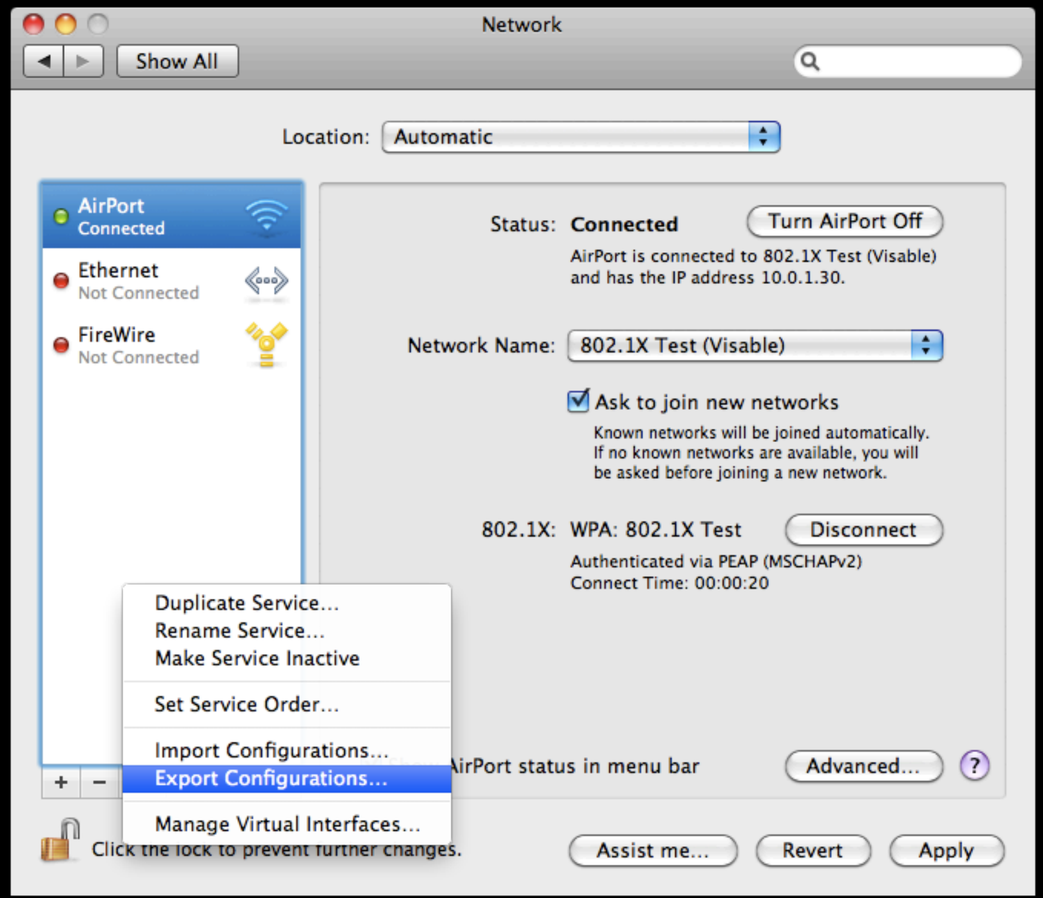
Mac OS X

- System Preferences import/export
- Import/export via command line

```
networksetup -import8021xProfiles
networksetup -export8021xProfiles
networksetup -export8021xUserProfiles
networksetup -export8021xLoginProfiles
networksetup -export8021xSystemProfile
```

- Associate identity to profile

```
networksetup -settlsidentityonuserprofile
networksetup -settlsidentityonsystemprofile
```



Automating Profile Configuration

Example: Unique user/machine identity via EAP-TLS

- Import the user or machine identity (cert + private key)

```
/usr/bin/security import -x <identity> -k <system keychain> -f pkcs12 -P pass
```

- Import and trust the server certificate

```
/usr/bin/security add-trusted-cert -d -r trustAsRoot -p eap
-k <system keychain> <server cert>
```

- Import the 802.1X system profile (previously exported)

```
networksetup -import8021xProfiles
```

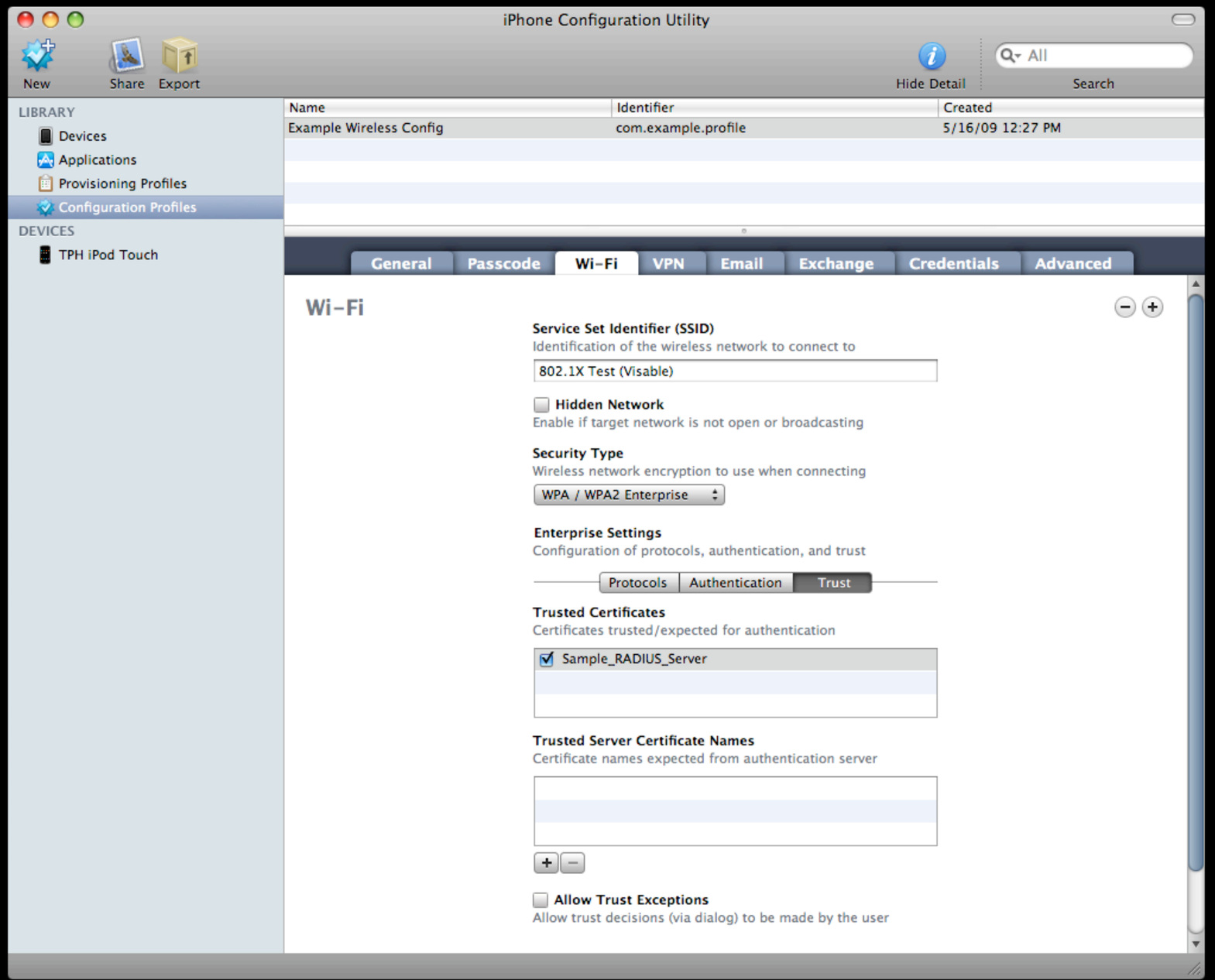
- Associate identity to system profile

```
networksetup -settlsidentityonsystemprofile
```

Imaging and 802.1X Profiles

- User profile
  - Does not image because of interface binding in “ByHost” preferences
  - Use networksetup to add a user profile
- System profile
  - Same credentials for all machines
  - Individual credentials configured via script
- Login window profile
  - Allows for multiple users
  - Most common for imaging

iPhone OS: 802.1X Deployment



Troubleshooting

General 802.1X Troubleshooting

Where is the problem occurring?

- Client logs (network and EAP)
- Authenticator logs
- Authentication server logs
- Directory server logs
- DHCP server logs
- Packet traces at various stages
  - tcpdump
  - WireShark for decoding

Supplicant

Authenticator

Authentication Server (RADIUS)

DHCP and Directory

Mac OS X Debug Logging

- System log file
- 802.1X (EAPoL) debug logs

```
defaults write /Library/Preferences/SystemConfiguration/com.apple.eapolclient LogFlags -int -1
```

- Files in /var/log/eapolclient/

- DHCP debug logs

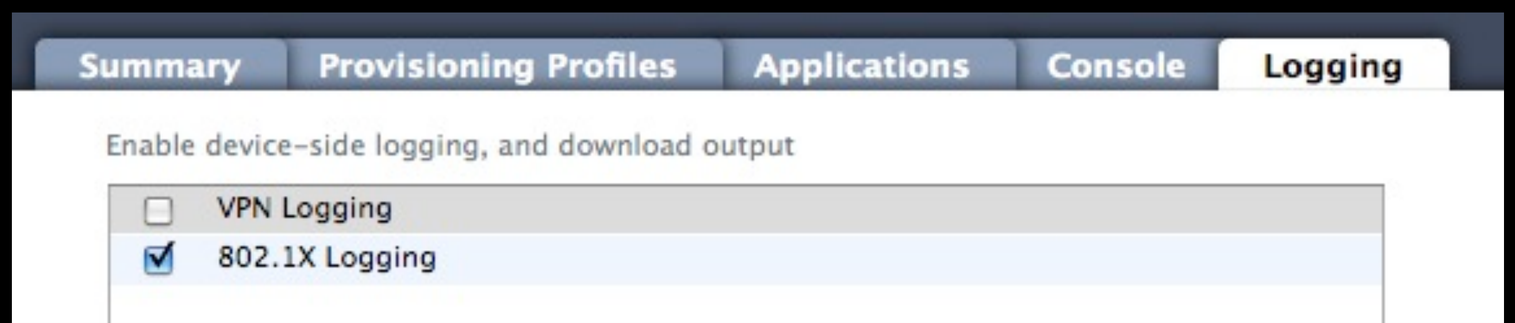
```
ipconfig setverbose 1
```

802.1X Logging for iPhone OS

- Log downloaded via iPhone Configuration Utility
- Enable debug log interface with defaults command:

```
defaults write com.apple.iPhoneConfigurationUtility EnableDebugLoggingInterface YES
```

- Check box to turn on 802.1.X debug logging



More Information

Nader Nafissi
Mac OS Server Product Marketing
macosxserver@apple.com

Documentation
Mac OS X Server Documentation
http://www.apple.com/server/documentation

Apple Training and Certification
http://training.apple.com

Related Sessions

iPhone Security Best Practices	Mission Wednesday 5:00PM
Scripting for System Administrators	Russian Hill Thursday 9:00AM

Labs

iPhone OS Security Lab	iPhone Lab D Thursday 5:00PM
Mac OS X Security Lab	OS X Lab A Wednesday 12:00PM

Summary

- 802.1X Supplicant built-in to Snow Leopard and iPhone OS
- Three Profile types in Snow Leopard for directory integration
- Snow Leopard deployment via imaging or profile import/export
- iPhone OS deployment via iPhone Configuration Utility

Q&A

WWDC Session Survey

You can rate your sessions on the WWDC Attendee Site.

Survey forms are located on each session description page at:

developer.apple.com/wwdc/attendee

WWDC09